ASSOCIATION OF PENSION LAWYERS

By email to: SARguidance@ico.org.uk

SAR guidance consultation
Regulatory Assurance Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

12 February 2020

Dear Sir/Madam

Consultation on the draft right of access guidance

Why are we writing to you?

I am writing on behalf of the APL International Sub-Committee of the Association of Pension Lawyers ("APL"). The purpose in writing this letter is to inform the ICO about the APL's interest in how the Right of Access guidance ("Guidance") will apply to UK pensions schemes and to provide some comments on this guidance. The APL is particularly interested in the application of the guidance to pension scheme trustees as data controllers who frequently have to deal with subject access requests ("SARs"), for example from a pension scheme member.

About the APL

By way of background, the APL represents members of the legal profession in the UK who specialise in pensions and pensions related law. It has over 1,100 members. It is a non-political, non-lobbying, not-for-profit organisation. A link to the APL website is as follows www.APL.org.uk. Activities undertaken by the APL on behalf of its members include the provision of technical legal support on both UK Government and EU legislative initiatives.

APL members (pensions lawyers) regularly advise persons and organisations with responsibility for running a wide range of different types of pension schemes. Such persons/organisations include trustees, employers, insurance companies and third party pensions administrators.

Our comments on the Guidance are as follows:

Preparatory steps for SARs (pages 3-15 of the Guidance)

Data controllers have a strict timeline for responding to a SAR. This should be reflected in contractual arrangements with processors. Data controllers should be

aware that processors may have sub-processors and sub-sub-processors, so collating and redacting information may be a lengthy process. While an exception to the requirements of SARs may apply, a consistent approach to contractual terms when engaging suppliers, vendors, or other processors is important. Likewise for processors, understanding how they can assist data controllers meet these obligations is key.

SARs can be made by the data subject in any form (phone, letter, email etc). Therefore a standard form is likely to be helpful, although we are not suggesting this is mandatory. An organisation may wish to take the request and input this into a standard form. This can then be shared back with the data subject in an acknowledgement letter confirming the organisations understanding of that request.

Taking into account the above points, we suggest that it would be useful to add the following preparatory steps to the list of examples in page 7 of the Guidance:

1. the review of contractual arrangements with data processors;
2. developing a policy or process for SARs;
3. which allocates responsibilities to specific people; and
4. preparing a standard SAR form to complete.

What should we consider when responding to a request? (pages 16-22)

The Guidance provides (at page 18) some helpful of examples of factors that may be relevant when determining whether or not a request is complex for the purposes of extending the time limit for responding. However, it suggests that having to rely on a processor to provide the information needed is not a relevant factor. While we have suggested including a review of contractual arrangements with data processors as a preparatory step on page 7 (see above), it is worth highlighting that trustees, as data controllers, will simply not have direct access to the data that their processors (e.g. third party administrators) hold on their own systems. It would be helpful if the Guidance could include some further flexibility in this area – for example:

1. making this a relevant factor to extend the timing for a response;
2. allowing a response to be sent in stages, i.e. a distinction between information that the controller has direct access to and information held by data processors; or
3. the ability to redirect the request to the data processor as a separate request.

On page 21 of the Guidance, reference is made to SARs being made by claims management companies on behalf of individuals. The Guidance suggests that the purpose for which the SAR is made does not affect its validity or the duty to respond (unless it is a manifestly unfounded or excessive request). Across the pensions (and financial services) industry we have recently seen a significant increase in claims management companies making fishing expeditions using SARs, often in bulk. In one recent case, a fake signature had been used and it transpired that the member was not even behind the request. The ICO and FAC issued a joint statement on 7 February regarding the sale of personal data to claims management companies. It would be helpful if the Guidance could specify that in the event of a breach of GDPR principles by a requester (where that is not the member) would render the request manifestly unfounded or allowing the controller to take into account the purpose (rather than just the context) for the request when determining its response.

How do we find and retrieve the relevant information? (pages 23-28)

We welcome the Guidance not requiring controllers to instruct staff to search their private emails and personal devices. In our experience, some trustees (e.g. those no longer working for the employer organisation) often use personal email addresses. The Guidance could helpfully include some examples of best practice to support this, for example ensuring that all trustees have organisation email addresses/devices that can be searched centrally or requiring all information to be deleted from private emails and personal devices as soon as practicable.

Special cases and health data (Pages 59-66)

More clarity and guidance around the restriction of disclosing health data for non-health professionals would be beneficial. Whilst these are likely to be exceptional cases, there may be relevant health data on a pension scheme member's file.

Disclosure of health data in response to a SAR is restricted unless the controller is satisfied that the health data has already been seen by or known by the individual; or, very broadly, an appropriate health professional's sign-off is obtained to the effect that disclosure would be reasonable and not cause serious harm to the physical or mental health of an individual.

Of course, most health data would fall outside the restriction as, due to the operation of the Access to Medical Records Act 1988, the individual will have seen the medical reports prepared about them, and they themselves may well have provided the health data to the employer/trustees to support an incapacity benefit claim.

However, the position is unclear where a trustee or employer has sought an independent medical opinion on an individual, perhaps to assess and provide a view on medical information provided by the member. Given the limited time to

respond to a SAR and the potential for severe consequences for non-compliance, trustees and employers may prefer to disclose all the information on file rather than rely on a restriction against disclosing this additional health data. However, so as to be able to disclose health data that is not seen or known by the member, specific sign-off against certain tests by an appropriate health professional is required. As currently drafted, circumstances could potentially arise where it is not clear whether disclosure of health data is appropriate, and trustees or employers may then be up against the clock to get medical sign-off to disclose.

The wording of the restriction may also cause confusion. The use of the phrase "known by" in the second part of the restriction is unclear and further guidance could be included about this. For example, does this refer to the member having actual knowledge of the existence of some health data on them, or could it just mean that the individual has been informed that the trustee or employer may consult its medical advisers about any health data provided by/in respect of the member?

General comments

Data controllers have one month to respond to a subject access request, but time doesn't start to run until receipt of any information requested to confirm the requester's identity (see page 16 of the Guidance). However, if the data controller wants to clarify the access request (to specify the information or processing activities), then this does not affect the timescale for responding (see page 23 of the Guidance). This does not appear particularly logical, and seems at odds with the wording of the GDPR which does not contain any such distinction.

As a general point, sometimes the Guidance isn't particularly specific. For example, checking the ID and authority of third parties making access requests on behalf of data subjects. In places, this may be because the GDPR is itself isn't detailed. It would be helpful if the Guidance were to signpost readers to the relevant legislation in each section. The Pensions Regulator usually does this in guidance or codes of practice – and so does some of the other ICO guidance (such as the new special category data guidance).

Finally, we would welcome your thoughts on how best we can engage with the ICO for assistance so that the APL can inform its members about the Guidance as it develops and once it is issued.

Please respond to the writer of this letter at:

Address: Mayer Brown International LLP, 201 Bishopsgate, London EC2M 3AF

Direct Line: [redacted]
Mobile:
Email:

ASSOCIATION OF PENSION LAWYERS

Yours faithfully

[redacted]

For and on behalf of the APL International Sub-Committee